ACTIVE VERIFICATION OF BOOT FIRMWARE

ABSTRACT

Techniques are described for generating and actively verifying a boot code associated with a peripheral device of a computer system to prevent potential security threats the boot code may introduce into the computer system. The techniques for generating boot code entail generating the boot code from a high-level programming language using a verification application program interface (API). The API aids in generating a certificate, which is associated with the boot code in that the certificate describes operation of the boot code. After generating the boot code and associated certificate, the two are loaded onto a memory module of the peripheral device. Once the peripheral device is connected to the computer system, the computer system may retrieve the boot code and certificate. The computer system utilizes techniques to actively verify the boot code by performing a security check on the boot code in accordance with the associated certificate. Finally, the computer system executes the boot code based on a result of the security check.